# Too Much Information: Questioning Security in a Post-Digital Society

**Lizzie Coles-Kemp**
ISG, Royal Holloway
University of London
Egham, TW20 0EX, UK
lizzie.coles-kemp@rhul.ac.uk

**Rikke Bjerg Jensen**
ISG, Royal Holloway
University of London
Egham, TW20 0EX, UK
rikke.jensen@rhul.ac.uk

**Claude Heath**
Media Arts, Royal Holloway
University of London
Egham, TW20 0EX, UK
claude.heath@rhul.ac.uk

## ABSTRACT

Whilst user- and people-centered design are accepted routes for digital services, they are less commonly used in the design of technologies that control access to data and the security of information. The ubiquity of both technology and programmes such as "digital by default" as well as the weaving of digital systems into the everyday fabric of society, create an environment in which people and technology become enmeshed. Such an environment might be termed "post-digital" and its security is dependent on a people-centered approach to its design. In this paper we present a study that uses critical design techniques coupled with critical security analysis to examine how security might be approached in a post-digital context. We call for a paradigm shift towards a people-centered security practice and using a case study then make practical recommendations as to how this shift might be achieved.

### Author Keywords

post-digital; post-digital security; lived experience; critical security design

### CCS Concepts

•**Security and privacy** → *Social aspects of security and privacy;* •**Human-centered computing** → *User studies;*

## INTRODUCTION

In the study and practice of technological security, the mantra "users are the weakest link" has been hard to disrupt and it reflects how people are often problematised when technological security is practised. From this perspective, people are regarded as a point of weakness, as a vulnerability to be exploited by attackers and malicious code, rather than as a source of strength; a position that, in the last few years, has been called into question by the UK's National Centre for Cyber Security (NCSC) [73]. Adams and Sasse [2] started to disrupt this narrative twenty years ago with their seminal paper *Users are Not the Enemy* and work in this tradition inspired a shift in the focus of national security guidance in the UK [72]. However, sociotechnical studies are still at the margins of technological security research and practice. Yet the widespread adoption of digital technology across society, digital by default modes of service delivery and the embedding of smart devices into everyday scenarios have woven issues of technological security into day to day life. This interweaving of the digital into the fabrics of society is termed by Cramer [29] as "post-digital". The post-digital brings with it the need for renewed forms of security where the links between human, societal and technological securities are a clear part of the analysis and design. In this paper, we use the term *"post-digital security"* for forms of sociotechnical security that address issues of trust, identity, privacy and security in post-digital contexts and societies through identity management, human relations and trust as well as technological security mechanisms.

In this paper, we present a case study that deploys a critical approach to examining security in a post-digital scenario, and reflect on how such an approach can be used to transform current security practice. Critical design is dialogic, perspective-shifting, creates holistic understandings and is reflexive [7]. The case study is designed using these principles and in its data analysis uses four critical security questions posited by Smith [82], a political theorist, to reflect upon what the data tell us about post-digital security practice.

As a start point, we call for three shifts in security practice to better address the post-digital:

- Shifting from telling people what makes them secure, towards discussing with them what their concerns are and what they regard as secure.
- Shifting from treating people as passive recipients of security awareness training, towards their becoming active participants in post-digital security learning.
- Shifting from "one size fits all" engagement techniques used for all groups within an organisation, towards the adaptation of engagement styles to each group.

In the literature review below, we examine how usable security scholarship and together with the wider HCI scholarship that relates to the security of people, communities and societies help us to facilitate this shift.



*CHI'20,* April 25–30, 2020, Honolulu, HI, USA



ACM ISBN 978-1-4503-6708-0/20/04.
DOI: https://doi.org/10.1145/3313831.3376214

## RELATED LITERATURE

The importance of designing usable and people-centered security is a clear theme in the technological security scholarship [42, 32]. In early work, Zurko [92] called for usability testing to be applied to secure systems, security models to be developed for user-friendly systems and for user needs to be considered as a primary design goal in security system design. This work has continued over the last two and a half decades and some of this scholarship is represented below.

### Scholarship into Practice

In the UK, HCI's usable security scholarship has been an important factor in encouraging a policy-driven shift towards people-centered security design and practice [73]. For example, in 2019 the NCSC in the UK launched guidance titled *You Shape Security* [64]. The breadth of this guidance reflects how usable security has inspired a wide range of sociotechnical security research. The guidance is primarily developed from UK people-centered security research and includes references to the authors' creative security research [25].

The *You Shape Security* guidance is primarily written for security practitioners: both those who design approaches to technical security within organisations and those who deploy and manage those approaches [46]. The guidance focuses on the message that for people to engage and comply with security technologies and practices, there has to be a clear benefit to them [77]. Yet it also recognises that identifying and agreeing upon such benefits is complex, requires negotiation and will differ between people. The guidance focuses on five types of engagement methods that security practitioners can use when engaging with different parts of an organisation to discuss and agree the relevant benefits of technology and as well as the concomitant security. These methods are:

- *Security incident and near miss reporting*: identified as a way for security practitioners to specify the areas in which engagement might be needed.
- *Surveys*: to capture the senses of security and the different concerns across an organisation. This brings to the fore methods of surveys and mass-interview techniques [78, 47].
- *Conversations with people*: to be used by security practitioners to engage with people and to listen to their concerns as well as impart specialist knowledge. This technique is informed by security dialogues research [5].
- *Creative narratives*: this technique foregrounds the narratives of everyday experiences of security [38, 57].
- *Creative engagement techniques*: a family of techniques [25] designed to question understandings of security in any given context and to promote spaces in which alternative perspectives on security can be heard.

In the following subsections, we set out the background HCI and sociotechnical security research literature that underpins this guidance. The breadth of this literature reflects the many different aspects of HCI that have influenced the direction of security practice.

### Trust and Technological Security

*You Shape Security* guidance has the building of trust relationships at its core, showing how security as both a technology and a service rely on many forms of trust. User-centered security is sometimes also referred to as trust user experience (TUX) [14] emphasising this. Whilst trust has long been cited as fundamental to a successful society [59], it does not carry a uniform meaning across all disciplinary positions. This is highlighted by Mollering [61], who outlines three schools of thought on trust: trust as reason, trust as routine and trust as reflexive. These are all tied to different disciplinary frameworks, ranging from psychology and a rational choice perspective, e.g. [45], to economic theories of trust focusing on limiting risk exploitation [86], along with broader sociological theorising on trust [56].

Whilst there have been calls for broader, sociological conceptualisations to be included in information security's understanding of trust [41, 79], much usable security research takes a psychological position on trust, one where trust is a rational choice – a decision – rather than a social construction. Moreover, trust in the digital context is problematic [84] – not least because the social norms and cultural practices that are needed to support trust interactions are harder to identify in online environments. The difficulty of mapping the social norms of the physical world with those experienced in the online world is exacerbated by online anonymity [60]. Anonymity creates the possibility of being able to violate social norms in online behaviours without being held accountable in the physical world. The difficulty of reading and interpreting such norms in online interactions, is, for example, one of the factors exploited in phishing attacks [34]. Nevertheless, it is argued that trust in online environments is possible [87] and usable security researchers have long argued that trust is a central component of effective security [41, 71, 53].

In a post-digital context, trust is formed as much by the interactions taking place around the technology as by the elements that form the digital interaction [51, 65]. A post-digital security therefore needs sociological understandings of trust to anticipate security responses and actions. Such a security also requires an understanding of the embodied sense of trust and technology to complement and contextualise the more traditional notion of trust in components [1] and trust in the transactions between those components [43]. This is because "[t]rust in everyday life is a mix of feelings and rational thinking" [56].

In summary, sociotechnical security research has examined primarily examined trust in technological components and transactions between those components. A post-digital security needs to also further develop understandings of embodied senses of trust and trust as a sociological reality in order to shape and anticipate the patterns of enmeshed sociotechnical technical practices.

### Challenges with Compliance

Encouraging people to follow security rules and policies is an important aspect of security practice and is a key focus for the security practitioner community. Understanding barriers to the following of security rules has been a persistent

line of enquiry in usable security scholarship. Renaud [70] highlighted that complex technological controls have a higher risk of not being complied with. She also demonstrates that environmental factors such as work stress, lack of clarity in security policies, and unrealistic task demands, all contribute to increasing the risk of accidental non-compliance. Unrealistic task demands have been explored as a key reason for non-compliance, with Blythe [16] terming these demands "response costs" and pointing out that the cost for people can be time, money and effort.

Research has highlighted that poorly designed security technology and badly implemented security programmes lead to a 'compliance overhead' [11] and that the true cost of this overhead is rarely calculated [47]. It is asserted that the true cost of ill-fitting security – that which does not meet the needs of people – is difficult to assess, because compliance is not a single behaviour [16] and because there are a great many factors that influence compliance. Blythe [16] lists these factors as:

- Self-efficacy which is an individual's belief about their own ability to perform a security task or exert an influence over it.
- Social influence which is the extent to which an individual's behaviour is influenced by others.
- Attitude towards the task.
- Perceived susceptibility towards a security threat against which the task is designed to protect.
- Perceived severity of the threat.
- Response efficacy which is the extent to which a task is regarded as an adequate response to the threat.
- Response cost which is the time, money and effort required to deploy the task.

Sasse et al.'s [47] research also shows that complex password rules not only impact on an individual's productivity but can also lead to security workarounds. Some usable security scholars, however, argue that workarounds are not necessarily an inferior option [8]. For example, Woltjer's research [90] shows that workarounds differ as to whether they are innovative security practices that run parallel to the security policies, or whether they are trade-offs that reduce security in favour of efficiency. It has been further argued that 'shadow security practices' – those that do not conform with security policy but that nevertheless provide security – are indeed a form of people-centered security design [53]. Workarounds and divergent security practices can result from a lack of common practice and usage goals. Karlsson [50] argues that the deployment of technology and the removal of face-to-face interactions can engender conflicted situations in which security practices will diverge. Research [6, 5] indicates that security practice therefore needs to pay careful attention to dialogue and engagement techniques as methods that can build the necessary common understandings and identify conflict as well as consensus around technology goals.

In summary, the usable security scholarship on compliance and workarounds provides important lessons for post-digital security. As this literature shows, non-compliance and divergent security practices are more likely when people have different understandings of the usage and benefit of technology. In summary, the lessons from studies of compliance highlight the need to communicate benefit of technology use if safe and secure practices are to follow. The communication of benefit is not a one-way dissemination of information. Post-digital security will need to build new understandings of not only benefit but also what it means to be secure in a digital context.

#### Security as a Contested Concept

A main theme in usable security scholarship has been towards making existing expert security knowledge comprehensible and usable to people. Such literature rarely focuses on everyday, non-expert conceptualisations of security, choosing instead to consider expert conceptualisations. Moreover, in information security terms, this builds on the belief that security knowledge held at "the top" is also the "correct" knowledge and that this knowledge will naturally produce effective information security policies and practices. By contrast, the importance of understanding everyday or "ground-up" forms of security has been recognised in wider security studies which have used the term "security from below" [24, 33] to argue for security policies about people rather than institutions [17]. This encompasses social, cultural, economic and political notions of protection. Wolff [89], a security scholar, made the observation that the purpose of security policies is simultaneously accepted and contested. This is because conceptualisations of security are many and varied [89] partly because different communities foreground different objects that need to be protected. For example, Nissenbaum [66] and Hansen and Nissenbaum [44] point out that computer security prioritises the protection of technology and data, foregrounding the threats to these elements accordingly; state security will focus on the protection of the state and sovereignty, foregrounding those threats accordingly. Similarly, citizens will focus on the threats to themselves and their kin and friendship networks [83], in a form of everyday security that differs from the security concerns of the state or security specialists. These meanings also evolve and change over an individual's lifetime [48].

The ground-up perspective is essential if post-digital security is to resonate with everyday lived experience. In order to represent everyday lived security experience, observed practices 'in the wild' [74, 37] need to be identified and understood. Studies of practices in the wild show that people engage with technological security not in isolation but as part of everyday technological practices [36]. Security practices in the wild are potentially challenging to the more orthodox conceptualisations of technological security as the emerging security concerns are often different to and sometimes conflict with expert understandings of technological security [26]. Everyday security practices [37] are partly grounded in the everyday security concerns of the individual and responded to through a routinisation and everyday practices [26, 31].

Understanding how everyday routines and rhythms create a sense of security are important in a post-digital context, where the boundaries between people and technology are blurred. HCI research that focuses on understanding the security of

people and how that relates to technology (rather than vice versa) is essential to better understand this socio-material relationship. Research grounded in HCI's ethnographic, situated traditions [35] are important for developing an understanding of the security of people. Such work is a bridge to HCI scholarship that focuses on human relational responses to security. Examples of HCI scholarship that look at the use of social relationships as a response to technological security issues include: Vines et al.'s [88] and Sleeper et al.'s [81] work on financial security, Ogbonnaya-Ogburu et al.'s [67] and Mentis et al.'s [58] work on safe digital inclusion and Corbett and Le Dantec's [27] work on trust and digital civics. Vines et al.'s [88] work shows how financial security, technological security and human security are intertwined and also foregrounds the relevance of socio-materiality in relation to feelings of security. Ogbonnaya-Ogburu et al.'s [67] work shows how access to services is far more complex than simply having technological availability and that feelings of insecurity shape online practices. Corbett and Le Dantec [27] reflect on the importance of trust relationships and its relevance to the successful deployment of technology.

In summary, by connecting technological security scholarship with the scholarship that is more focused on social and human relational responses to technological security, a *post-digital security* scholarship emerges where security is no longer simply framed as an individualistic issue and activity but also as an issue that affects communities and as an activity in which people co-operate. Acts of co-operation and community response are a necessary response to security issues in post-digital contexts.

## SECURITY IN A POST-DIGITAL CONTEXT: A CASE STUDY

In this section, we present a case study designed to critically evaluate what sort of security is both needed and achieved in a post-digital setting. Molotch [62], a sociologist, who studied security in the wild argued: "The bottom line for the security of anything – hardware, software, airports or subways – is the same. Dig deep into how people actually operate in the everyday including the ways they already solve problems, particularly those to do with safety." The approach taken in this case study is designed to enable participants to dig deep by creating a safe-space in which participants can create a detailed narrative of everyday technology use and critically examine what they discover.

The use of IoT for the monitoring of people was set as the context within which the participants worked. This is a context in which the security of people and the security of technology are physically and technologically interwoven [68]. In order to compare different framings of security in this post-digital context, two very different perspectives were selected; security practitioners and healthcare service providers. In the case of the security practitioners, the use of IoT to monitor staff was the given scenario. In the case of the healthcare service providers, the use of IoT by patients to self-manage health conditions was the given scenario. The case studies illustrate how the themes of the literature review: issues of trust, compliance and workarounds and competing conceptualisations of security can play out in a post-digital scenario.

A physical (LEGO) modelling approach was chosen as the main engagement method because it creates "rich pictures" [63], thus, encouraging participants to reflect on the ways in which technology is woven into their everyday practices. A critical security engagement challenges the assumptions about what it means to be secure and how security is achieved. The approach was deployed using critical design principles [7] that foster a reflexive, dialogic approach and that promote a holistic understanding of security situated in a particular context. This approach promotes an understanding of technologies that are attentive to the wider political economy of technology deployment [40, 39].

### Study Design and Methods

The study approach used can be situated amongst an established body of related scholarly literature [20, 75, 21, 80] and commercial practice [69] and is based on "creative security" [38], a technique for participative and playful engagement. Creating a *safe space* where participants can explore their concerns and imagine alternative futures is an important principle of creative engagement. Trust is fundamental to this type of participatory engagement [23] and much can be learned from the trust principles of participatory practice in a civic setting, see for example the work in [18, 23].

The case study has one common study design but is enacted in two parts: (1) an engagement with security practitioners and (2) an engagement with healthcare service providers. As noted above, this is a context in which the security of people and the security of technology are physically and logically interwoven in a post-digital setting. In terms of participant selection: security practitioners were recruited in order to explore technology protection practices in a post-digital setting; that healthcare service providers were recruited so to the security practices of a group interested in the use of IoT but whose focus is patient care not technological protection. This participant recruitment was intended to give both a 'top-down' and 'ground-up' perspective of post-digital security.

#### *Session Structure*

We used the following standardised engagement protocol with both participating groups. After introducing the study, we ran a short brainstorming session where participants responded to prompts constructed to encourage the critical examination of the security of the context (see Table 1).

Participants used story sheets to capture their ideas in response to such prompts. Then we introduced the LEGO modelling component where participants worked on the scenarios and issues raised during the initial brainstorming segment.

The term "security" was left very broad to draw out the broader themes from the literature review. The post-digital scenario was designed to encourage participants to engage with these themes and enabled researchers to explore how the importance of trust relationships, compliance and workarounds and the negotiation of alternative conceptualisations of security emerge in a post-digital scenario. The prompts, questions and scenarios were deliberately chosen to facilitate this broad discussion.

| | Prompts |
|---|---|
| **Prompt 1** | "What is smart monitoring technology?" |
| **Prompt 2** | "What services do smart monitoring technology provide?" |
| **Prompt 3** | "What security issues does smart monitoring technology introduce and why?" |
| **Prompt 4** | "What are the possible responses to those security issues introduced by smart monitoring technology, and whom do they benefit and disbenefit?" |

**Table 1. Prompts used during brainstorming sessions.**

*Security Practitioners*: 55 security practitioners were recruited to participate in a workshop at the CyberUK conference in 2016. The security practitioners were split into ten groups with five to six participants per group. The groups were deliberately set so that in each group there was a mixture of different types of security practice such as auditing, security architecture design, risk and governance. Each group worked around a table and groups appointed a facilitator, a scribe to make notes and the remaining three to four participants were model makers. Each group was given a box of LEGO and a grey LEGO baseboard. Each group was also given a set of instructions, as shown in Figure 1, for building the model together with a suggestion as to how the different coloured bricks might be used; for example: one colour to represent data, one colour to represent digital hardware and one colour to represent physical environments. The groups were also given Post-It notes, blank design cards and paper tape that could be used by the group to annotate the model.

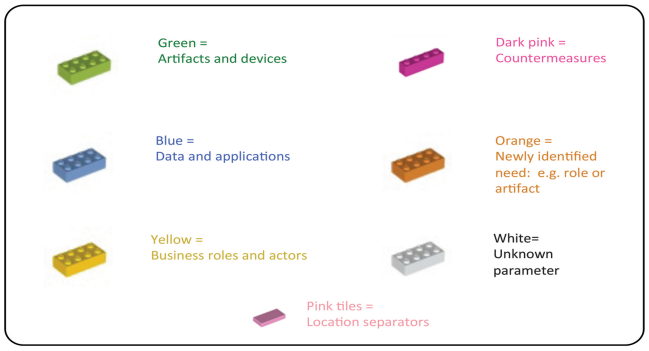


**Figure 1. The instructions given to participants show the colour schema for the LEGO bricks that they were invited to use.**

To stimulate discussion, each group was given the same Dilbert cartoon about staff monitoring [3]. In the cartoon, Dilbert is surprised to learn that his every movement is monitored and processed through data gathered by a comprehensive array of sensors in his workplace, including CCTV, eye-movement tracking software, and biometrics.

Having read the cartoon and discussed it, each group was asked to use the LEGO kits provided to them to model the technical, security and social implications of IoT monitoring as they saw it. Each group was asked to start by creating a scenario that included IoT monitoring and populating this with actors (represented by LEGO figures), using the schema of LEGO bricks to represent the environment, as shown in Figure 1: noting the physical, technical and data elements. Each group worked on their model for approximately 45 minutes by working through the prompts and provocations (please see Table 1) and then concluded with a summary of the opportunities and challenges that arose in this context together with ideas as to how the security issues of IoT monitoring might be responded to.

*Healthcare Service Providers*: Participants in the healthcare service provider workshop were recruited with the help of the Health Foundry in London. 15 people took part. Four groups of three to four people were set-up. As with the security practitioners each group was provided with a LEGO kit comprising a set of instructions, LEGO bricks, a grey baseboard, Post-It notes and blank design cards. Each group appointed a facilitator and a scribe, and sat around a table. Each group was asked to consider the use of IoT to monitor health conditions.

Instead of a cartoon, a scenario was presented to stimulate discussion. As with the security practitioners, each group was asked to consider the technical, security and societal implications of IoT monitoring as they saw it. Each group was asked to start by creating a scenario that included the use of IoT to monitor a health condition in the home. This scenario was modelled by using a schema of LEGO bricks to represent the environment: noting the physical, technical and data elements. The scenario was then populated with actors represented by LEGO figures. Each group worked on their model for approximately 45 minutes by working through the prompts and provocations (please see Table 1) and then concluded with a summary of the opportunities and challenges that arose in this context together with ideas as to how the security issues of IoT monitoring might be responded to.

### *Data Gathering and Analysis*

The data was gathered, processed and stored under ethical approval from the academic institution. Data was generated in the form of LEGO models, annotations made by individual participants, facilitator observations, notes of collaborative outcomes from the brainstorming, and final group-feedback contributions. Additional data gathered for analysis included: 1) hand-written annotations placed on models by participants, and text gathered from the story sheets, 2) investigator notes, and 3) photographs of the models both individually and as a collage. It was not possible to audio-record the security practitioner session because some preferred not to be recorded due to the nature of their job but it was possible to record the healthcare service provider session. The recording of this session was transcribed and then the photographic documentation was combined with the transcriptions. We used inductive thematic analysis as described by Braun and Clarke [19] and two researchers independently coded the themes and then jointly resolved thematic conflicts. We included analysis of the visual data using Gillian Rose's analytical approach to understanding visual data [76]. The themes were then interrogated from the perspective of Smith's four critical security questions [82] in order to identify how the workshop findings challenge assumptions and understandings related to information security practice. These four questions are [82]:

- Who or what needs to be secured?
- What is doing the securing?
- Why is the subject being secured?
- Who or what is the subject being secured from?

In this way, a critical security perspective was maintained during analysis.

A short illustrated report was produced from each workshop that outlined the workshop conclusions. The report was sent to a representative of each participant group for discussion and feedback. Written feedback was given by the participant groups and was incorporated into the final analysis and findings.

## FINDINGS

The following themes were identified from the analysis:

- Security Issues. Much of the response from the security practitioners focused on the inherent threat of not being in control. This manifested itself in a sense of being overwhelmed with the volume of data, and also of not being able to create a protected and stable perimeter around the technology itself. This relates to the theme of trust in technology, highlighting the potential threat produced by a destabilising lack of trust in security technology capabilities.
- Who Secures? Both groups questioned central premises, such as: who or what is making these contexts secure? Both groups concluded that the technological responses were only a part of any answer to this question, and that social interaction plays an equally important and necessary securing function. This theme sheds further light on why 'workarounds' might appear in order to mitigate deficits in security technology capabilities, and highlights the importance of human and social relationships in securing these contexts.
- Benefits and Disbenefits. Both groups identified that establishing, agreeing and communicating the benefits of IoT monitoring were important processes for the establishment of why security was needed and in what form. It is through this dialogic process that alternative conceptualisations of security are both identified and reconciled.

The questioning of security brought forward not only issues of technological security but also human and societal security. There were also issues of job security, in the case of security practitioners, and also questions of organisational security. The discussions in both groups around "who or what is doing the securing?" show how these securities become enmeshed in each other and must be responded to holistically if post-digital contexts are to be secure.

### *What security issues are introduced and why?*

Both groups felt threatened by the unknown. Analysing the responses from the critical security perspective of "who or what is the threat?", both groups felt threats from technology that had been implemented to support and help. For example, security practitioners reported feeling overwhelmed with data. The different groups focused on the immense difficulties of managing complex oversized data flows and that the monitoring of data had added to this complexity. For the participants, the data is complex, composed of lots of input streams – none of which are complete and which have different levels of verification. "Too much information, distracted, bad decisions" reads one of the labels added to a model (Figure 3).

Being deluged in data was also regarded as a potential threat to the mental health of those whose job it is to use that data to protect environments: "The data is everywhere and coming from all angles" (Figure 2). There was a strong sense that this was an environment that security specialists did not properly understand, and for that reason it was difficult to see how the environment could be harnessed for the good. One annotation read: "Internet of Things = Unknown".

The threat that emerged from the opening up of the environment was a particular concern: "IoT third parties are able to open gates". This opening up of the environment can also result in accidental disclosure. Security practitioners conceived of situations where this might come from attackers mixing disparate streams of data, including IoT monitoring, to filter and make sense of data to achieve further intelligence on attack goals. This sense of openness was also echoed by the healthcare service providers, who argued that there were "too many logon opportunities" in an IoT monitoring infrastructure.

Healthcare service providers also focused on potential threats from the unknown, but from the perspective of a lack of legibility of the data not from the perspective of too much data. It was felt that lack of transparency and accountability (both perceived and actual) might act as a barrier to wider adoption of health monitoring tools, even where there are recognised potential benefits to patient health. Healthcare service providers argued that different perspectives need to be taken into account in order to develop a fuller understanding of the entire problem space around IoT in healthcare. They argued that this multi-perspectival view could reduce the number of unknowns by identifying not only a wider range of issues but also a wider range of potential responses and greater resilience, as was vividly represented in the avenues converging on the patient in the 'Perspectives on Care' model (Figure 4).

### *Who or What is Doing The Securing?*

Both groups engaged critically with the question of what would offer protection in this scenario. Security practitioners were better able to state what was not doing the securing rather than what was. Their responses showed that they viewed technological controls as being less effective. They argued that the sheer volume of data could overwhelm and make the security controls less effective in this context. Some data pathways remained manageable to the security practitioners but faced with the complexity of the situation, small blue loose LEGO parts, representing 'Open source unverified data', were scattered liberally over the model to reflect the difficulty of identifying every data path (see Figure 2). It was said that data was everywhere and that there was no possibility at all of mapping it, both in the LEGO model and also in security practice. In a sense, the limitations of modelling in LEGO the complexity of post-digital contexts were also a metaphor for the difficulties of managing the security implications of IoT monitoring.

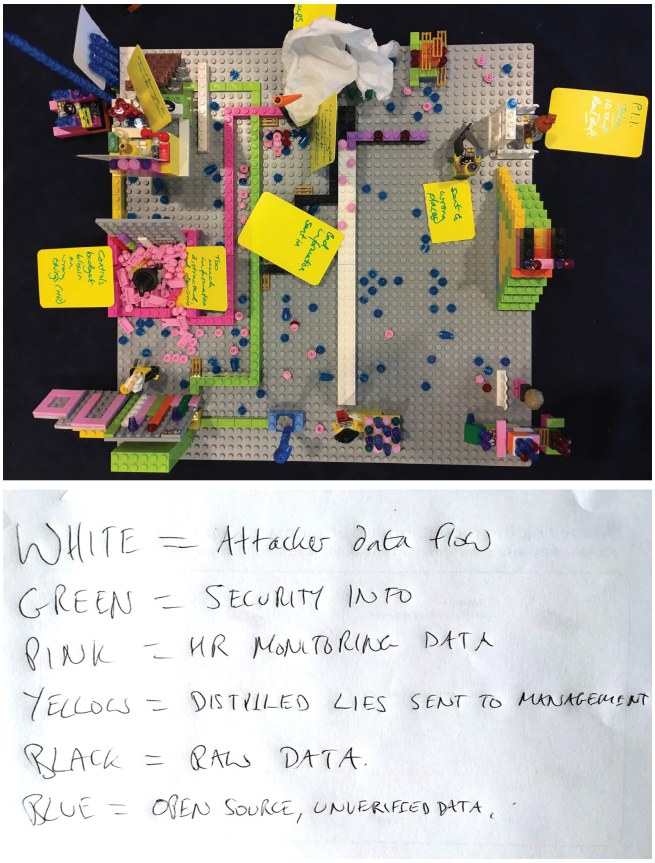


**Figure 2. A security practitioner model: 'Too Much Information'. The modellers created their own handwritten colour-code (below) for information flows seen in the overhead view (above). This shows how these flows interact with one another. Pink tiles and smaller pieces denote 'HR Monitoring data' captured within an organisation recording the activities of its own workforce.**

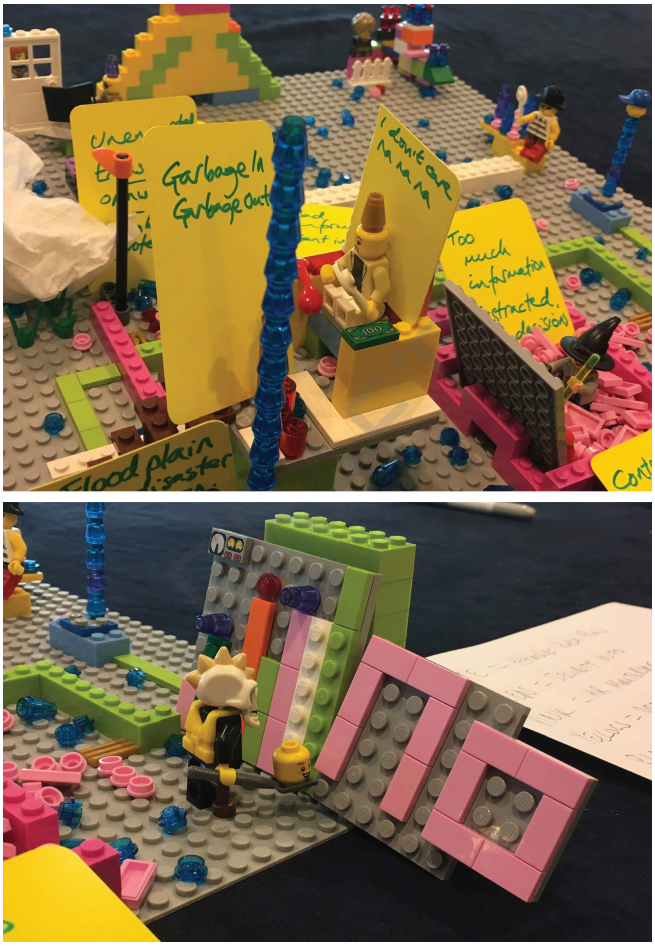


**Figure 3. Details of the 'Too Much Information' security practitioner model. A manager sits amidst enormous stacks of blue data, annotations reading 'I don't care, Na, na'; 'Garbage In - Garbage Out'; 'Controls budget blown on wrong things'; 'Too much information, distracted, bad decisions.' An analyst is mired in loose pink data ('HR Monitoring data'). Below, an analyst attempts to make sense of the data using bar charts, with little success: pink tiles read: 'No'.**

It was explained that the superfluity of data was a problem for security practice, as such practice relies on being able to identify flows of data in order to verify and protect those flows with technological controls. As a result, IoT monitoring can create as many (if not more) risks than it resolved because the technological controls were unable to identify and respond to issues of unauthorised data access and unauthorised modification of either the primary data flows or the additional data flows introduced through monitoring (or both).

Security practitioners also revealed a sense of frustration that these difficulties could not be communicated to management. Their reflections also showed a sense of a lack of agency, in that security specialists felt they could not push back on the use of IoT monitoring. This sense of lack of agency was articulated as follows: "Controls budget; blown on the wrong things", and "Yellow [bricks] = distilled lies sent to management."

By contrast, the healthcare service providers focused on the importance of different types of accessibility and saw accessibility as a means of securing people and technology and building community and individual resilience. Healthcare service providers stated that an approach to technological design was needed that made data use transparent to users, informed by active consent and clear accountability and that this would secure people. Technology, not yet available, needed to be in place so that trust could be built through regular feedback and updates to users on how their data is being used.

Healthcare service providers also highlighted another weakness with the technical controls, not mentioned by security practitioners. Whilst the security practitioners focused on the superfluity of the data, the healthcare service providers were worried that some data would be blocked or unavailable due to problems related to interoperability between systems, and across the different data types being worked with. Focus therefore also had to be on delivering fully supported data sharing infrastructures as a means to secure the scenario.

### *Benefits and Disbenefits of IoT Monitoring*

Both groups felt that if harnessed correctly, monitoring could increase creativity and open up opportunities for new ways of working as shown in Figure 4. However, both groups were critical of what was actually being secured, and why.


**Figure 4. A healthcare service provider model: 'Perspectives on Care'. In the centre is the user of IoT devices and services in healthcare, surrounded by several avenues (family, GP, CCG (Clinical Commissioning Group), dietitian, cardiologist, pharmacist, insurance firms, gyms, etc) holding data about that person and which may be relevant to their healthcare. Below, the sub-group of healthcare service providers build and discuss their model, while other sub-groups work on theirs nearby.**

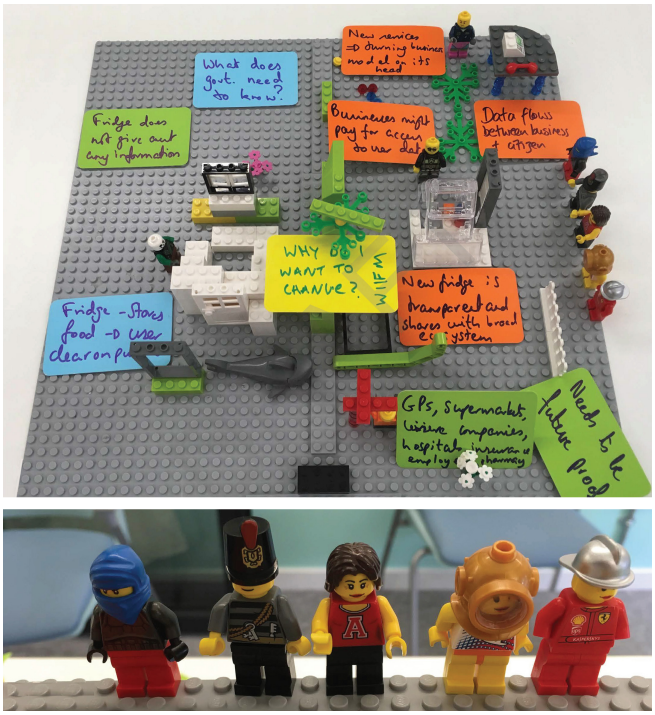


**Figure 5. A healthcare service provider model: 'The Future Fridge.' Left, the initial state, a user with a standard white fridge. Right, the after state, where the user has adopted an internet-connected 'smart' fridge. Annotations on this model included: 'Demonstrable benefit: What's the use to me?'; 'Who is seeing the data?'; 'How can we safeguard vulnerable people?'; 'Want the IoT landscape to operate in an ethical way'. Below: The five prospective users of healthcare IoT (on a spectrum of fitness, health, and early adoption). Other annotations read: 'Fridge stores food->user clear on it's purpose,' and 'Fridge does not give out any information.' 'Businesses are scared of making a mistake'; 'Need open standards e.g. Creative Commons license'; 'Is there a role for Blockchain in IoT security/data'; 'Need flexibility so that what you create today is relevant tomorrow.'**

Security practitioners felt that the monitoring scenario was one that opened up the possibility of wider social risks. One security practitioner annotated their model with the reflection "Staff sue company for discrimination/human rights", a risk stemming from personally identifiable information becoming compromised. Healthcare service providers considered how this risk could be reduced through the use of monitoring needs to be culturally sympathetic and supportive, and the interpretation of the resulting data needs to be both pragmatic and consultative with that community. Healthcare service providers also felt that public and private stakeholders in healthcare delivery must be prepared to have their existing business models questioned and opened up. Transactions with the user will need to be renegotiated in order to make the basis of the relationship (and exchange) clearer.

Security practitioners put forward the view that IoT monitoring data could be harnessed to improve morale – relieving workplace inefficiencies, inconveniences and frustrations, and potentially leading to innovations and alternatives being offered to these common problems. The end result, it was said, would be improved resilience and defence against data attack. Similarly, healthcare professionals thought that IoT monitoring for health could "bring the world" to older people whose data is vulnerable: explaining the benefits of IoT technologies was seen as an important means of gaining 'buy-in' from employees. Organisations, the security practitioner groups asserted, did not do enough to focus on the benefits to employees and to identify creative uses for the data. Poor use of monitoring data followed as a result, with detrimental effects on staff and the creation of scenarios in which data was vulnerable to attack. A similar point was also made by the healthcare service providers, who strongly put forward the view that the benefits of monitoring need to be made clear before people would be willing to part with their data.

## DISCUSSION

In this discussion we examine how a critical approach to security design differs from an affirmative one and reflect on the roles for each. We then examine why a critical approach is useful in post-digital contexts. Finally, we outline the changes

a critical approach can bring to security practice and how the HCI community can further strengthen such an approach.

### Affirmative and Critical Approaches

The NCSC guidance [64] is a strong example of a shift towards people-centered security practice and design. Nevertheless, the framing of people-centered security still typically foregrounds an affirmative design where expert-developed principles of technology security are the basis for engagement between security practitioners and communities of technology users. In contrast, the method deployed in the case study offers a critical rather than an affirmative perspective. This approach creates spaces in which the expert framing of post-digital security issues can be challenged and a "ground-up" perspective can be developed that frames the post-digital security challenges from the perspective of those groups into whose lives the digital is woven.

Much of the background literature section represents research that is focused on ensuring that technological security works more effectively and efficiently by being more compatible with human practice. However, whilst such affirmative positions are important for the design of reliable technology and services, such research gives little or no space for alternative conceptualisations of post-digital security or security issues. In order to achieve the goals of initiatives such as *You Shape Security* [64], and to be fully people-centered, there has to be space for such alternative conceptualisations and also for the opportunity to question the value and assumptions of digital security in any given setting.

In the case study, the security practitioners critically reflected on the difficulties of working with and analysing what they described as "too much data". Their concern was not only as to whether the human operators are able to cope with this volume of data, but also whether the technological controls themselves would be capable of processing this much data in any kind of useful way. In this scenario, critical reflection is opened up, not only to human practice but also to technological design itself. Thus, in response to the critical security question "Who or what is doing the securing?", the response we observed is that security is not achieved through the gathering of large amounts of data from tracking devices and other similar technologies. Instead, the critical reflections from the security practitioners highlight that technical controls on their own are severely limited in a post-digital context, and that human interactions promoting trust-building and resilience are important to security practice.

The security practitioners also reflect that the challenge of too much data is a message that is not welcomed by the leadership of organisations. As a result of this wider political context, a fiction had to be created and re-presented to an organisation's management, a fiction regarding who or what constitutes the threat, and which represents the potency of data to respond to that threat. The critical reflection revealed the acknowledged role of these self-imposed fictions in reaffirming managerial assumptions about the efficacy of existing security technologies and practices.

The healthcare service providers critically reflected on who or what needs to be protected, and who or what is the threat. They call for transparency, indicating that the service providers and technology companies are a perceived source of threat themselves. As a result, they argue that service provider business models should be opened up for review. The call for transparency is a recurrent theme when trust in both the technology and the providers decreases and the demand for greater control increases [91]. However, further critical reflection is required as Kizilec's [54] research has also shown that too much transparency can result in the degradation of trust.

Both groups critically reflected on whether the technological controls are able to provide sufficient protection. Consequently, the groups considered how the wider social, political and economic context might play a part in the security of IoT monitoring. In both groups, there was a recognition that if the narrative relating to the use of IoT monitoring is not felt to be positive in nature, and if the design of the services does not clearly benefit the people being monitored, there are significant risks from people resisting such monitoring. This critical reflection acknowledges the risks that flow from either claiming benefits that are not present or from promoting a negative frame that imposes monitoring. Consequently, the dialogue used to frame technology benefits is an important part of security practice.

Such critical reflections provide a multi-perspectival view of what protections are needed and what protections are most effective. With this understanding relevant security policies and principles can be established and these may run counter to orthodox security practices and principles.

### Coming to Terms with Post-Digital Security

As the case study shows, the challenges of controlling and protecting data are amplified in the post-digital context, where the use of digital technology in everyday life has become inseparable from wider social and cultural practices. The post-digital poses challenges for how we think about post-digital security because it becomes harder to separate people into "them" and "us", as the case study demonstrates. As the evidence from the security practitioners reveals, technologically controlling all points of access in a post-digital context is an ineffective strategy, is in part what makes this type of separation harder. The findings from the case study suggest that just as post-digital technology is enmeshed within wider cultural and social practices, so too must security become a techno-socio-cultural response. However, the post-digital poses a challenge for security because the extent to which a context is post-digital depends in part on how people experience the technology. One context can be post-digital for one person but not for another resulting in multiple meanings and understandings of post-digital security. For example one person can be oblivious to sensor technology, whilst someone else may regard it as an intrusive surveillance device. As a result, the post-digital is not universally felt or experienced; as the post-digital advances, more is asked of people-centered security design and of those who inform and guide security practice.

The notion of a post-digital world thus challenges the separation between the physical/material and the virtual/immaterial,

which has also been highlighted by scholars in the field of geography [52, 4] and more widely (e.g. [55, 49]). As Cramer [29] notes, the "post" in "post-digital" does not necessarily point to a time *after* digital technology or, as others have suggested (e.g. [15, 13]), a rejection of digital technology – what has been termed "the hipster's dilemma" [85]. Rather, Cramer [29] argues that the term "post-digital" refers to the ways in which digital technology has become so intrinsically interwoven into the fabrics of societies and into people's daily lives that it no longer makes sense as a standalone concept. To this end, digitalisation has already happened [28].

Whilst much of the thinking related to the post-digital has emerged from within digital arts and humanities and critical theory [13, 12, 30, 22], the post-digital requires a rethinking of security and of the processes of securing. Indeed, the post-digital has a direct impact on how we understand and relate to notions of post-digital security. Collapsing the digital/non-digital divide requires an understanding of where technological security is an embodied experience as much as a technological solution; an understanding of technological and individual security that allows for a broad conceptualisation of security as well as a reflexive research approach. "Post-digital security" therefore necessitates a discussion of whether post-digital security has any meaning as a separate notion, or whether the protection of technology and information has become so intermingled with the protection of people and society that distinguishing between the two is impossible. In other words, in a post-digital society, technological security rests upon the protection of people, and vice versa.

### Implications for Security Practice

Usable security research, in common with other branches of HCI, often struggle to identify and understand the limits of technology [10]. As Baumer [9, 10] discusses, HCI has a paucity of research on design for reflection and design that acknowledges the limits of technology. However, as the above case study illustrates, understanding the limits of security technology and practice is key to developing effective security strategies for post-digital environments.

Following this case study, the following practical changes should be considered to security practice:

- Inclusion of critical security questions: information security risk assessment should include critical security questions of the type posed by Smith [82] when assessing risk to data and technology in order to identify the communities affected by these risks and the sources of those risks.

- Inclusion of ground-up as well as top-down perspectives: security policies and processes should include ground-up perspectives as well as top-down perspectives on security practice in order to ensure that the security issues addressed are representative of the communities using the technologies.

- The processes for setting and deploying security policies should include opportunities for identifying both consensus and conflict related to security goals and the benefits of technology in a particular setting.

- Designing discussion fora and opportunities to learn from alternative conceptualisations of security and its practice in order to continuously develop a holistic and fluid understandings of post-digital security.

These are practical responses to the paradigm shift that is called for in the Introduction. For in offering a means of bringing together different understandings of security, new responses can be created and appreciated.

Such an approach offers the possibility of a more holistic security practice, one in which several branches of HCI scholarship play a fundamental role. The security practitioner group focuses on the system and management perspective whereas the healthcare service providers focus on the perspective of the individual and of resilient collective action. By putting together both perspectives, a more complete perspective is achieved and, interestingly, one perspective might suggest responses to challenges raised in the other perspective. For example, the security practitioner's view that the volume of data would overwhelm the technological controls, is countered by the healthcare service providers who propose that agreeing principles of use and sharing respond to those challenges by fostering more trusted, resilient contexts of use. Thus a people-centered approach to security practice is introduced which encourages notions of security to be challenged; the aim of which is to arrive at consensus as to the benefits and meanings of security in context.

## CONCLUSIONS

Questioning security and what it means to be secure in post-digital contexts is key to identifying where there are differences in outlook and where these might lead to differences in practice. Security practice then becomes not about imposing a singular view of security on the use of technology but of identifying and working with multiple views. The findings also suggest a multi-perspectival approach is needed to avoid the generic, universal approach to security that tends to dominate. Looking at post-digital security practice through this lens, NCSC's *You Shape Security* guidance [64] becomes a collection of tools to question the meanings of security in a given context, converge on a set of understandings and respond to those understandings. This is a radical departure from the way that such approaches are typically framed: as techniques for affirming the principles of technological security through compliant practice.

## ACKNOWLEDGMENTS

We would like to thank our participants and the hosting institutions for taking part and thank the NCSC for the input from the Sociotechnical Security Group. Without their efforts, enthusiasm and energy this work would not have been possible. Coles-Kemp's and Heath's contribution was funded by the "Everyday safety-security for everyday services" fellowship programme funded by EPSRC award EP/N02561X/1.

The dataset for this paper can be found at https://doi.org/10.17637/rh.11528166

## REFERENCES


[1] Alfarez Abdul-Rahman and Stephen Hailes. 1998. A distributed trust model. In *Proceedings of the 1997 workshop on New security paradigms*. ACM, 48–60.

[2] Anne Adams and Martina Angela Sasse. 1999. Users are not the enemy. *Commun. ACM* 42, 12 (1999), 41–46.

[3] Scott Adams. 2014. Managing Employee Data the Dilbert Way. https://dilbert.com/strip/2014-05-11. (2014). Accessed: 2019-09-19.

[4] James Ash, Rob Kitchin, and Agnieszka Leszczynski. 2018. Digital turn, digital geographies? *Progress in Human Geography* 42, 1 (2018), 25–43.

[5] Debi Ashenden and Darren Lawrence. 2016. Security dialogues: Building better relationships between security and business. *IEEE Security & Privacy* 14, 3 (2016), 82–87.

[6] Debi Ashenden and Angela Sasse. 2013. CISOs and organisational culture: Their own worst enemy? *Computers & Security* 39 (2013), 396–405.

[7] Jeffrey Bardzell and Shaowen Bardzell. 2013. What is critical about critical design?. In *Proceedings of the SIGCHI conference on human factors in computing systems*. ACM, 3297–3306.

[8] Steffen Bartsch and Martina Angela Sasse. 2012. How users bypass access control and why: the impact of authorization problems on individuals and the organization. (2012).

[9] Eric PS Baumer. 2015. Reflective informatics: conceptual dimensions for designing technologies of reflection. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*. ACM, 585–594.

[10] Eric PS Baumer and M Silberman. 2011. When the implication is not to design (technology). In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2271–2274.

[11] Adam Beautement, M Angela Sasse, and Mike Wonham. 2009. The compliance budget: managing security behaviour in organisations. In *Proceedings of the 2008 New Security Paradigms Workshop*. ACM, 47–58.

[12] David M Berry. 2014. Post-digital humanities: Computation and cultural critique in the arts and humanities. *Educause* 49, 3 (2014), 22–26.

[13] David M Berry and Michael Dieter. 2015. Thinking postdigital aesthetics: art, computation and design. In *Postdigital aesthetics*. Springer, 1–11.

[14] Colin Birge. 2009. Enhancing research into usable privacy and security. In *Proceedings of the 27th ACM international conference on Design of communication*. ACM, 221–226.

[15] Ryan Bishop, Kristoffer Gansing, Jussi Parikka, and Elvia Wilk. 2016. *Across and beyond: a transmediale reader on post-digital practices, concepts and institutions*. Sternberg Press and Transmediale eV.

[16] John M Blythe, Lynne Coventry, and Linda Little. 2015. Unpacking security policy compliance: The motivators and barriers of employees' security behaviors. In *Eleventh Symposium On Usable Privacy and Security ({SOUPS} 2015)*. 103–122.

[17] Monica den Boer and Jaap de Wilde. 2008. The viability of human security. (2008).

[18] Alex Bowyer, Kyle Montague, Stuart Wheater, Ruth McGovern, Raghu Lingam, and Madeline Balaam. 2018. Understanding the family perspective on the storage, sharing and handling of family civic data. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. ACM, 136.

[19] Virginia Braun and Victoria Clarke. 2006. Using thematic analysis in psychology. *Qualitative research in psychology* 3, 2 (2006), 77–101.

[20] Peter Bürgi and Johan Roos. 2003. Images of strategy. *European Management Journal* 21, 1 (2003), 69–78.

[21] Peter T Bürgi, Claus D Jacobs, and Johan Roos. 2005. From metaphor to practice in the crafting of strategy. *Journal of Management Inquiry* 14, 1 (2005), 78–94.

[22] Kim Cascone. 2000. The aesthetics of failure: "Post-digital" tendencies in contemporary computer music. *Computer Music Journal* 24, 4 (2000), 12–18.

[23] Rachel Elizabeth Clarke, Jo Briggs, Andrea Armstrong, Alistair MacDonald, John Vines, Emma Flynn, and Karen Salt. 2019. Socio-materiality of trust: co-design with a resource limited community organisation. *CoDesign* (2019), 1–20.

[24] Alexandra Abello Colak and Jenny Pearce. 2009. 'Security from Below' in Contexts of Chronic Violence. *IDS Bulletin* 40, 2 (2009), 11–19.

[25] Lizzie Coles-Kemp. 2018. Practising Creative Securities. https://bookleteer.com/collection.html?id=28. (2018). Accessed: 2019-08-19.

[26] Lizzie Coles-Kemp and René Rydhof Hansen. 2017. Walking the line: The everyday security ties that bind. In *International Conference on Human Aspects of Information Security, Privacy, and Trust*. Springer, 464–480.

[27] Eric Corbett and Christopher A Le Dantec. 2018. Going the distance: Trust work for citizen participation. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. ACM, 312.

[28] Geoff Cox. 2014. Prehistories of the post-digital: Or, some old problems with post-anything. *A Peer-Reviewed Journal About* 3, 1 (2014).

[29] Florian Cramer. 2015. What is 'Post-digital'? In *Postdigital aesthetics*. Springer, 12–26.

[30] Florian Cramer. 2016. Post-digital literary studies. *MATLIT: Materialities of Literature* 4, 1 (2016), 11–27.

[31] Stuart Croft and Nick Vaughan-Williams. 2017. Fit for purpose? Fitting ontological security studies 'into' the discipline of International Relations: Towards a vernacular turn. *Cooperation and conflict* 52, 1 (2017), 12–30.

[32] Robert E Crossler, Allen C Johnston, Paul Benjamin Lowry, Qing Hu, Merrill Warkentin, and Richard Baskerville. 2013. Future directions for behavioral information security research. *computers & security* 32 (2013), 90–101.

[33] Martijn Dekker and Mient Jan Faber. 2008. Human security from below in a Hobbesian environment. *Security & Hum. Rts* 19 (2008), 37.

[34] Rachna Dhamija, J Doug Tygar, and Marti Hearst. 2006. Why phishing works. In *Proceedings of the SIGCHI conference on Human Factors in computing systems*. ACM, 581–590.

[35] Paul Dourish. 2006. Implications for design. In *Proceedings of the SIGCHI conference on Human Factors in computing systems*. ACM, 541–550.

[36] Paul Dourish and Ken Anderson. 2006. Collective information practice: Exploring privacy and security as social and cultural phenomena. *Human-computer interaction* 21, 3 (2006), 319–342.

[37] Paul Dourish, E Grinter, Jessica Delgado De La Flor, and Melissa Joseph. 2004. Security in the wild: user strategies for managing security as an everyday, practical problem. *Personal and Ubiquitous Computing* 8, 6 (2004), 391–401.

[38] Paul Dunphy, John Vines, Lizzie Coles-Kemp, Rachel Clarke, Vasilis Vlachokyriakos, Peter Wright, John McCarthy, and Patrick Olivier. 2014. Understanding the experience-centeredness of privacy and security technologies. In *Proceedings of the 2014 New Security Paradigms Workshop*. ACM, 83–94.

[39] Hamid Ekbia and Bonnie Nardi. 2015. The political economy of computing: the elephant in the HCI room. *interactions* 22, 6 (2015), 46–49.

[40] Hamid Ekbia and Bonnie Nardi. 2016. Social inequality and HCI: The view from political economy. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. ACM, 4997–5002.

[41] Ivan Flechais, Jens Riegelsberger, and M Angela Sasse. 2005. Divide and conquer: the role of trust and assurance in the design of secure socio-technical systems. In *Proceedings of the 2005 workshop on New security paradigms*. ACM, 33–41.

[42] Steven Furnell and Nathan Clarke. 2012. Power to the people? The evolving recognition of human aspects of security. *computers & security* 31, 8 (2012), 983–988.

[43] Diego Gambetta and others. 2000. Can we trust trust. *Trust: Making and breaking cooperative relations* 13 (2000), 213–237.

[44] Lene Hansen and Helen Nissenbaum. 2009. Digital disaster, cyber security, and the Copenhagen School. *International studies quarterly* 53, 4 (2009), 1155–1175.

[45] Russell Hardin. 2004. *Trust & Trustworthiness*. Russell Sage Foundation.

[46] Kirstie Hawkey, David Botta, Rodrigo Werlinger, Kasia Muldner, Andre Gagne, and Konstantin Beznosov. 2008. Human, organizational, and technological factors of IT security. In *CHI'08 extended abstracts on Human factors in computing systems*. ACM, 3639–3644.

[47] Philip G Inglesant and Martina Angela Sasse. 2010. The true cost of unusable password policies: password use in the wild. ACM.

[48] Simon L Jones, Emily IM Collins, Ana Levordashka, Kate Muir, and Adam Joinson. 2019. What is' Cyber Security'?: Differential Language of Cyber Security Across the Lifespan. In *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems*. ACM, LBW0269.

[49] Heekyoung Jung and Erik Stolterman. 2012. Digital form and materiality: propositions for a new approach to interaction design research. In *Proceedings of the 7th Nordic Conference on Human-Computer Interaction: Making Sense Through Design*. ACM, 645–654.

[50] Fredrik Karlsson, Martin Karlsson, and Joachim Åström. 2017. Measuring employees' compliance–the importance of value pluralism. *Information & Computer Security* 25, 3 (2017), 279–299.

[51] Tim Kindberg, Eamonn O'Neill, Chris Bevan, Vassilis Kostakos, Danaë Stanton Fraser, and Tim Jay. 2008. Measuring trust in wi-fi hotspots. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 173–182.

[52] Samuel Kinsley. 2014. The matter of 'virtual' geographies. *Progress in Human Geography* 38, 3 (2014), 364–384.

[53] Iacovos Kirlappos, Simon Parkin, and M Angela Sasse. 2014. Learning from "Shadow Security": Why understanding non-compliance provides the basis for effective security.

[54] René F Kizilcec. 2016. How much information?: Effects of transparency on trust in an algorithmic interface. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. ACM, 2390–2395.

[55] Paul M Leonardi, Bonnie A Nardi, and Jannis Kallinikos. 2012. *Materiality and organizing: Social interaction in a technological world*. Oxford university press on demand.

[56] J David Lewis and Andrew Weigert. 1985. Trust as a social reality. *Social forces* 63, 4 (1985), 967–985.

[57] Makayla M Lewis and Lizzie Coles-Kemp. 2014. Who says personas can't dance?: the use of comic strips to design information security personas. In *CHI'14 Extended Abstracts on Human Factors in Computing Systems*. ACM, 2485–2490.

[58] Helena M Mentis, Galina Madjaroff, and Aaron K Massey. 2019. Upside and Downside Risk in Online Security for Older Adults with Mild Cognitive Impairment. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. ACM, 343.

[59] John Stuart Mill and others. 1848. *The principles of political economy*. Vol. 2. Batoche.

[60] David R Millen and John F Patterson. 2003. Identity disclosure and the creation of social capital. In *CHI'03 extended abstracts on Human factors in computing systems*. ACM, 720–721.

[61] Guido Mollering. 2006. *Trust: Reason, routine, reflexivity*. Emerald Group Publishing.

[62] Harvey Molotch. 2013. Everyday security: Default to decency. *IEEE Security & Privacy* 11, 6 (2013), 84–87.

[63] Andrew Monk and Steve Howard. 1998. Methods & tools: the rich picture: a tool for reasoning about work context. *interactions* 5, 2 (1998), 21–30.

[64] NCSC. 2019. You Shape Security. https://www.ncsc.gov.uk/collection/you-shape-security. (2019). Accessed: 2020-01-04.

[65] Maria Nilsson, Anne Adams, and Simon Herd. 2005. Building security and trust in online banking. In *CHI'05 Extended Abstracts on Human Factors in Computing Systems*. ACM, 1701–1704.

[66] Helen Nissenbaum. 2005. Where computer security meets national security. *Ethics and Information Technology* 7, 2 (2005), 61–73.

[67] Ihudiya Finda Ogbonnaya-Ogburu, Kentaro Toyama, and Tawanna R Dillahunt. 2019. Towards an Effective Digital Literacy Intervention to Assist Returning Citizens with Job Search. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. ACM, 85.

[68] James Pierce. 2019. Smart Home Security Cameras and Shifting Lines of Creepiness: A Design-Led Inquiry. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. ACM, 45.

[69] Lego Serious Play. 2010. Open Source Introduction to Lego Serious Play. *Billund: Lego. Lokaliseret den* 7 (2010), 2013.

[70] Karen Renaud. 2011. Blaming noncompliance is too convenient: What really causes information breaches? *IEEE Security & Privacy* 10, 3 (2011), 57–63.

[71] Jens Riegelsberger, M Angela Sasse, and John D McCarthy. 2005. The mechanics of trust: A framework for research and design. *International Journal of Human-Computer Studies* 62, 3 (2005), 381–422.

[72] RISCS. 2017a. People are the Strongest Link. https://www.ncsc.gov.uk/speech/people–the-strongest-link. (2017). Accessed: 2019-09-12.

[73] RISCS. 2017b. Putting People First. https://www.riscs.org.uk/ciaran-martin-putting-people-first/. (2017). Accessed: 2019-09-12.

[74] Yvonne Rogers. 2011. Interaction design gone wild: striving for wild theory. *interactions* 18, 4 (2011), 58–62.

[75] Johan Roos, Bart Victor, and Matt Statler. 2004. Playing seriously with strategy. *Long Range Planning* 37, 6 (2004), 549–568.

[76] Gillian Rose. 2016. *Visual methodologies: An introduction to researching with visual materials*. sage.

[77] Angela Sasse. 2015. Scaring and bullying people into security won't work. *IEEE Security & Privacy* 13, 3 (2015), 80–83.

[78] Martina Angela Sasse. 2005. Usability and trust in information systems. Edward Elgar.

[79] Martina Angela Sasse, Sacha Brostoff, and Dirk Weirich. 2001. Transforming the "weakest link"– a human/computer interaction approach to usable and effective security. *BT technology journal* 19, 3 (2001), 122–131.

[80] Klaus-Peter Schulz and Silke Geithner. 2013. Creative Tools for Collective Creativity The Serious Play Method Using Lego Bricks. *Learning and Collective Creativity: Activity-Theoretical and Sociocultural Studies* (2013), 179–197.

[81] Manya Sleeper, Tara Matthews, Kathleen O'Leary, Anna Turner, Jill Palzkill Woelfer, Martin Shelton, Andrew Oplinger, Andreas Schou, and Sunny Consolvo. 2019. Tough Times at Transitional Homeless Shelters: Considering the Impact of Financial Insecurity on Digital Security and Privacy. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. ACM, 89.

[82] Graham M Smith. 2005. Into Cerberus' Lair: Bringing the Idea of Security to Light. *The British Journal of Politics & International Relations* 7, 4 (2005), 485–507.

[83] Daniel Stevens and Nick Vaughan-Williams. 2016. Everyday security threats: Perceptions, experiences, and consequences. (2016).

[84] Mariarosaria Taddeo. 2010. Trust in technology: A distinctive and a problematic relation. *Knowledge, Technology & Policy* 23, 3-4 (2010), 283–286.

[85] Claes Thorén, Mats Edenius, Jenny Eriksson Lundström, and Andreas Kitzmann. 2019. The hipster's dilemma: What is analogue or digital in the post-digital society? *Convergence* 25, 2 (2019), 324–339.

[86] Jan Tullberg. 2008. Trust-The importance of trustfulness versus trustworthiness. *The Journal of Socio-Economics* 37, 5 (2008), 2059–2071.

[87] Matteo Turilli, Antonino Vaccaro, and Mariarosaria Taddeo. 2010. The case of online trust. *Knowledge, Technology & Policy* 23, 3-4 (2010), 333–345.

[88] John Vines, Mark Blythe, Paul Dunphy, Vasillis Vlachokyriakos, Isaac Teece, Andrew Monk, and Patrick Olivier. 2012. Cheque mates: participatory design of digital payments with eighty somethings. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 1189–1198.

[89] Josephine Wolff. 2016. What we talk about when we talk about cybersecurity: security in internet governance debates. *Internet Policy Review* 5, 3 (2016).

[90] Rogier Woltjer. 2017. Workarounds and trade-offs in information security–an exploratory study. *Information & Computer Security* 25, 4 (2017), 402–420.

[91] Peter Worthy, Ben Matthews, and Stephen Viller. 2016. Trust me: doubts and concerns living with the Internet of Things. In *Proceedings of the 2016 ACM Conference on Designing Interactive Systems*. ACM, 427–434.

[92] Mary Ellen Zurko and Richard T Simon. 1996. User-centered security. In *NSPW*, Vol. 96. Citeseer, 27–33.